Ref. 1

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-258745

(43)Date of publication of application : 11.09.2002

(51)Int.CI. G09C 1/00
H04L 9/32

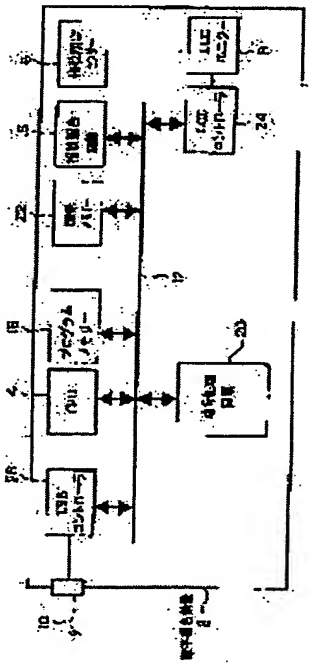
(21)Application number : 2001-061353

(22)Date of filing : 06.03.2001

(71)Applicant : SONY CORP

(72)Inventor : TSUKAMURA YOSHIHIRO
FUNABASHI TAKESHI

(54) DIGITAL SIGNATURE DEVICE



(57)Abstract:

PROBLEM TO BE SOLVED: To electronically sign only data which a signer has surely confirmed.

SOLUTION: A CPU 14 receives data of a check or the like, which should be electronically signed, through a USB cable 10 and supplies this document data to a liquid crystal monitor 8 to display a picture of the check. The signer puts his or her finger on a fingerprint collation sensor 6 after seeing this display to confirm contents. The fingerprint collation sensor 6 reads the fingerprint to generate its video signal, and a fingerprint collation circuit 18 identifies the signer on the basis of the fingerprint picture represented by this video signal. Then, the CPU 14 starts a cipher processing circuit 20 to supply the document data to the cipher processing circuit 20. The cipher processing circuit 20 generates hash values of the document data and uses a secret key out of a public key and the secret key, which have been preliminarily generated on the basis of a public cipher key system, to encipher the hash values. The CPU 14 outputs the result through the USB cable 10.

Ref. 1

対応なし、英抄

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－258745
（P2002－258745A）
(43)公開日　平成14年９月11日(2002.9.11)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
G09C	1/00	640	G09C	1/00	640B　5J104
H04L	9/32		H04L	9/00	673D
					673A

審査請求　未請求　請求項の数11　ＯＬ　（全６頁）

(21)出願番号　特願2001－61353(P2001－61353)

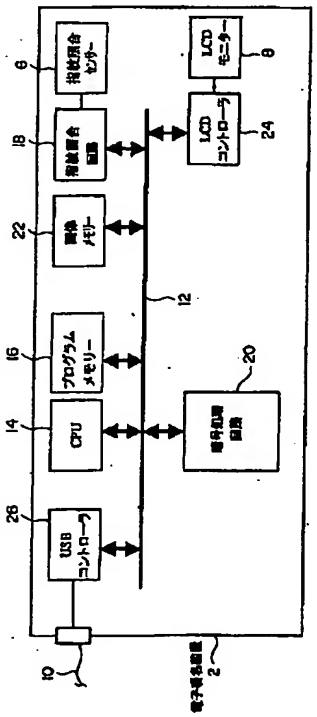
(22)出願日　平成13年３月６日(2001.3.6)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　塚村　善弘
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　船橋　武
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100089875
弁理士　野田　茂

Ｆターム(参考)　5J104 AA07 AA09 KA01 KA16 KA17
KA18 LA06 NA05 NA12

(54)【発明の名称】　電子署名装置

(57)【要約】
【課題】　確実に署名者が確認したデーターに対してのみ電子署名を行う。
【解決手段】　ＣＰＵ１４は電子署名を行うべきたとえば小切手のデーターをＵＳＢケーブル１０を通じて受け取り、同文書データーを液晶モニター８に供給して小切手の画像を表示させる。署名者はこの表示を見て内容を確認した上で、指紋照合センサー６上に指を配置する。指紋照合センサー６は指紋を読み取って指紋の映像信号を生成し、指紋照合回路１８は、この映像信号が表す指紋画像にもとづいて署名者の認証を行う。その後ＣＰＵ１４は、暗号処理回路２０を起動し、上記文書データーを暗号処理回路２０に供給する。暗号処理回路２０は同文書データーのハッシュ値を生成し、あらかじめ公開暗号鍵方式にもとづいて生成しておいた公開鍵と秘密鍵のうち、秘密鍵を用いて上記ハッシュ値を暗号化する。ＣＰＵ１４はこの結果をＵＳＢケーブル１０を通じて出力する。



1

【特許請求の範囲】

【請求項１】　署名者があらかじめ登録されている特定の人物であるか否かを判定する認証手段と、
電子署名を行うべきデーターを表す情報を出力する情報出力手段と、
前記電子署名を行うべきデーターからハッシュ値を生成するハッシュ値生成手段と、
公開鍵暗号方式にもとづく公開鍵および秘密鍵を生成する暗号鍵生成手段と、
前記暗号鍵生成手段が生成した前記秘密鍵を用いて、前記ハッシュ値生成手段が生成した前記ハッシュ値を暗号化するハッシュ値暗号化手段と、
署名者が登録されている特定の人物であると前記認証手段が判定した場合に、前記ハッシュ値暗号化手段が暗号化した前記ハッシュ値を出力するハッシュ値出力手段とを備えたことを特徴とする電子署名装置。

【請求項２】　前記認証手段は署名者のバイオメトリックスにもとづいて署名者があらかじめ登録されている特定の人物であるか否かを判定することを特徴とする請求項１記載の電子署名装置。

【請求項３】　前記認証手段は、署名者の指から指紋を読み取り、読み取った指紋があらかじめ登録されている指紋であるか否かを判定する指紋照合手段により構成されていることを特徴とする請求項１記載の電子署名装置。

【請求項４】　前記認証手段は、署名者の声紋にもとづいて署名者があらかじめ登録されている特定の人物であるか否かを判定することを特徴とする請求項１記載の電子署名装置。

【請求項５】　前記認証手段は、署名者が文字を書く際の筆圧の変化にもとづいて署名者があらかじめ登録されている特定の人物であるか否かを判定することを特徴とする請求項１記載の電子署名装置。

【請求項６】　前記認証手段は、署名者がパスワードを入力するパスワード入力手段と、同パスワード入力手段を通じて入力されたパスワードが、あらかじめ登録されているパスワードに一致するか否かを判定する照合手段とを含んで構成されていることを特徴とする請求項１記載の電子署名装置。

【請求項７】　前記情報出力手段は、液晶表示装置を含み、前記電子署名を行うべきデーターを文字情報として前記液晶表示装置に表示することを特徴とする請求項１記載の電子署名装置。

【請求項８】　前記情報出力手段は、スピーカまたはイアホーンを含み、前記電子署名を行うべきデーターを音声情報としてスピーカーまたはイアホーンを通じて出力することを特徴とする請求項１記載の電子署名装置。

【請求項９】　前記情報出力手段は、前記電子署名を行うべきデーターを映像信号として出力する出力端子を含むことを特徴とする請求項１記載の電子署名装置。

2

【請求項１０】　前記情報出力手段は、前記電子署名を行うべきデーターを音声信号として出力する出力端子を含むことを特徴とする請求項１記載の電子署名装置。

【請求項１１】　前記情報出力手段は、液晶表示装置を含み、前記電子署名を行うべきデーターを文字情報として前記液晶表示装置に表示し、前記認証手段は、前記液晶表示装置の表示部に配設された筆圧センサーを含み、署名者が同筆圧センサー上で文字を書く際の筆圧の変化にもとづいて署名者があらかじめ登録されている特定の人物であるか否かを判定することを特徴とする請求項１記載の電子署名装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は電子署名を行う装置に関するものである。

【０００２】

【従来の技術】電子署名は、文書などが署名を行った者により作成されたものであり、かつ他者により改ざんされていないことを証明する技術として、近年の通信ネットワークを通じた電子決済の普及などとともに重要性が増している。図５はこのような従来の電子署名装置の一例を示す構成図である。図５に示した電子署名装置１０２は、指紋照合器１０４（特開２０００－１８５９４号公報）とパーソナルコンピュータ１０６（パソコン１０６ともいう）により構成されている。電子署名を行う場合には、署名者はまずパソコン１０６を操作して、電子署名を行うべきたとえば小切手１０８のデーターにもとづいて小切手１０８の画像をパソコン１０６の画面に表示させる。署名者はこれを見て小切手１０８の内容を確認し、内容に間違いがない場合には、指紋照合器１０４の指紋照合センサー１１０上に自身の指１１１を配置する。これにより指紋照合器１０４は指紋を読み取って指紋の画像データーを生成し、指紋照合器１０４にあらかじめ登録されている、上記署名者の指紋の画像データーと比較して、上記読み取った指紋が登録されている指紋か否かを判定する。

【０００３】この判定結果が正の場合には、指紋照合器１０４は、あらかじめ公開暗号鍵方式にもとづいて生成しておいた公開鍵と秘密鍵のうち、秘密鍵をケーブル１１２を通じてパソコン１０６に出力する。パソコン１０６側では、この秘密鍵を指紋照合器１０４から受け取ると、上記小切手１０８のデーターにもとづいてハッシュ値を生成するとともに、同ハッシュ値を、指紋照合器１０４からの秘密鍵を用いて暗号化する。なお、ハッシュ値の暗号化は指紋照合器１０４で行う構成でもよく、その場合、パソコン１０６は、生成したハッシュ値を指紋照合器１０４に送り、指紋照合器１０４はパソコンからのハッシュ値を上記秘密鍵により暗号化してパソコン１０６に出力する。

【０００４】これにより電子署名が完了し、暗号化され

たハッシュ値は通信ネットワークや記憶媒体を通じて受け取り手に渡されることになる。ハッシュ値を受け取った側では、上記署名者の公開鍵を用いてハッシュ値を復号するとともに、上記小切手１０８のハッシュ値を、上記パソコン１０６と同じアルゴリズムによって生成する。そして、生成したハッシュ値と、復号したハッシュ値とが一致した場合には、小切手１０８は間違いなく上記署名者により署名されたものであると判定できる。

【０００５】

【発明が解決しようとする課題】しかし、このような電子署名装置１０２は、よりセキュリティーを高めるべく、以下の点で改良が望まれる。すなわち、パソコン１０６がたとえば通信ネットワークに接続されている場合には、通信ネットワークを通じて何らかの形でパソコン１０６にプログラムが組み込まれる可能性がある。そして、そのプログラムにより、上述のように小切手１０８からハッシュ値を生成する段階で小切手１０８の金額を１００万円から１２０万円に変更されるといったことが起こり得る。

【０００６】このような変更が加えられると、署名者は１００万円と記載された小切手１０８をパソコン１０６の画面で確認して署名を行ったにもかかわらず、１２０万円の小切手に対して署名をしたことになり、損失を被る結果となる。本発明はこの種の問題を解決するためになされたもので、その目的は、確実に、署名者が確認したデーターに対してのみ電子署名が行われるようにした電子署名装置を提供することにある。

【０００７】

【課題を解決するための手段】本発明は上記目的を達成するため、署名者があらかじめ登録されている特定の人物であるか否かを判定する認証手段と、電子署名を行うべきデーターを表す情報を出力する情報出力手段と、前記電子署名を行うべきデーターからハッシュ値を生成するハッシュ値生成手段と、公開鍵暗号方式にもとづく公開鍵および秘密鍵を生成する暗号鍵生成手段と、前記暗号鍵生成手段が生成した前記秘密鍵を用いて、前記ハッシュ値生成手段が生成した前記ハッシュ値を暗号化するハッシュ値暗号化手段と、署名者が登録されている特定の人物であると前記認証手段が判定した場合に、前記ハッシュ値暗号化手段が暗号化した前記ハッシュ値を出力するハッシュ値出力手段とを備えたことを特徴とする。

【０００８】本発明の電子署名装置では、情報出力手段が、電子署名を行うべきデーターを表す情報を出力するので、署名者はこの出力結果にもとづいて電子署名を行うべきデーターの内容を確認することができる。そして、ハッシュ値生成手段は上記電子署名を行うべきデーターにもとづいてハッシュ値を生成する。その後、ハッシュ値暗号化手段は、暗号鍵生成手段が生成した秘密鍵を用いてハッシュ値生成手段が生成したハッシュ値を暗号化し、ハッシュ値出力手段は、署名者が特定の人物であると認証手段が判定した場合に、ハッシュ値暗号化手段が暗号化したハッシュ値を出力する。このように本発明では、情報出力手段が内容確認のために情報を出力するデーターと、ハッシュ値生成手段がハッシュ値の生成に用いるデーターとは常に同一であり、したがって、かならず署名者が確認したデーターに対してのみ電子署名が行われる。

【０００９】

【発明の実施の形態】次に本発明の実施の形態例について図面を参照して説明する。図１は本発明による電子署名装置の一例を示すブロック図、図２の（Ａ）は電子署名装置を示す外観図、（Ｂ）は液晶モニターに表示された文書の一例を示す平面図である。図２の（Ａ）に示したように、本実施の形態例の電子署名装置２は、ケース状あるいはカード状などの単一の装置収容体４の表面に指紋照合センサー６および液晶モニター８（ＬＣＤモニター）を配置して構成されている。指紋照合センサー６は、指紋照合センサー６上に配置された指２８から指紋を読み取り、指紋の映像信号を生成する。液晶モニター８は、ＵＳＢケーブル１０を通じて供給された、電子署名を行うべき文書のデーターにもとづいて同文書の画像を表示するために設けられている。

【００１０】より詳しくは、電子署名装置２は図１に示したような構成となっている。すなわち、電子署名装置２はバスライン１２により接続されたＣＰＵ１４およびプログラムメモリー１６を含み、ＣＰＵ１４はプログラムメモリー１６に格納されたプログラムデーターにもとづき動作し、電子署名装置２全体の制御などを行う。

【００１１】バスライン１２にはまた、指紋照合回路１８および暗号処理回路２０が接続されている。指紋照合回路１８は、たとえばＬＳＩ（Ｌａｒｇｅ　Ｓｃａｌｅ　Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）から成り、指紋照合センサー６からの映像信号にもとづいて、同映像信号が表す指紋画像と、あらかじめ画像メモリー２２に格納されている指紋のテンプレート画像とを、たとえばパターンマッチングなどを行って比較し、指紋照合センサー６により読み取られた指紋があらかじめ登録されている指紋か否かを判定する。なお、指紋照合回路１８は指紋照合センサー６とともに本発明に係わる認証手段、すなわち指紋照合手段を構成している。

【００１２】暗号処理回路２０（本発明に係わるハッシュ値生成手段、暗号鍵生成手段、ハッシュ値暗号化手段）は、たとえばＬＳＩから成り、文書データーのハッシュ値の生成、ならびに公開鍵暗号方式にもとづく公開鍵および秘密鍵の生成を行い、さらに上記ハッシュ値を上記秘密鍵によって暗号化する。

【００１３】上記液晶モニター８（本発明に係わる情報出力手段）は、液晶コントローラー２４を通じてバスライン１２に接続され、液晶コントローラー２４による制御のもとで、ＣＰＵ１４からバスライン１２を通じて送

5

られてくるデーターにもとづき文書を表示する。上記ＵＳＢケーブル１０は、ＵＳＢコントローラー２６を通じてバスライン１２に接続されており、ＵＳＢケーブル１０を介してＣＰＵ１４が外部機器との間でデーターの授受を行えるようになっている。

【００１４】次に、このように構成された電子署名装置２の動作について説明する。ここでは、一例として電子署名装置２はＵＳＢケーブル１０を介して不図示のパソコンに接続されており、電子署名を行うべき文書データーは同パソコンから供給され、また結果も同パソコンに出力するものとする。電子署名装置２により電子署名を行う場合、署名者はまず上記パソコンを操作して、電子署名を行うべきたとえば小切手のデーターを電子署名装置２に出力させ、また電子署名の実行を指示させる。これにより電子署名装置２では、ＣＰＵ１４が上記文書データーをＵＳＢケーブル１０、ＵＳＢコントローラー２６、ならびにバスライン１２を通じて受け取り、プログラムメモリー１６に格納するとともに、バスライン１２および液晶コントローラー２４を通じて液晶モニター８に出力し、図２の（Ｂ）に示したように、小切手の画像を画面に表示させる。

【００１５】署名者はこの表示を見て小切手の内容を確認し、内容に間違いがない場合には、指紋照合センサー６の上に自身の指２８を配置する。指紋照合センサー６は指８が配置されると指８から指紋を読み取って指紋の映像信号を生成し、指紋照合回路１８に出力する。そして、指紋照合回路１８では、この映像信号が表す指紋画像と、あらかじめ画像メモリー２２に格納されている指紋のテンプレート画像とを、たとえばパターンマッチングなどを行って比較し、指紋照合センサー６により読み取られた指紋が登録されている指紋か否かを判定する。この判定結果が正の場合、指紋照合回路１８はその旨をＣＰＵ１４に通知する。

【００１６】これによりＣＰＵ１４は、暗号処理回路２０を起動するとともにプログラムメモリー１６に格納されている文書データーを暗号処理回路２０に供給する。そして、暗号処理回路２０は、供給された文書データーのハッシュ値を生成し、あらかじめ公開暗号鍵方式にもとづいて生成しておいた公開鍵と秘密鍵のうち、秘密鍵を用いて上記ハッシュ値を暗号化する。

【００１７】ＣＰＵ１４はこの暗号化されたハッシュ値を受け取り、上述のように署名者が認証されているため、ハッシュ値出力手段として動作して、ＵＳＢコントローラー２６からＵＳＢケーブル１０を通じて上記パソコンに出力する。これにより電子署名が完了し、暗号化されたハッシュ値は、その後、パソコンから通信ネットワークや記憶媒体を通じて受け取り手に渡されることになる。

【００１８】このように本実施の形態例では、液晶モニター８が表示する文書画像のデーターと、暗号処理回路

6

２０がハッシュ値の生成に用いるデーターとは常に同一であり、したがって、かならず署名者が確認したデーターに対してのみ電子署名が行われる。

【００１９】本実施の形態例では、署名者指紋により認証を行うとしたが、署名者の認証は様々な技術により行うことができ、たとえば署名者の網膜など他のバイオメトリックスにもとづいて署名者があらかじめ登録されている特定の人物であるか否かを判定するようにすることも可能である。また、署名者の声紋を利用して認証を行うことも可能である。

【００２０】さらに、電子署名装置２に筆圧センサーを組み込んで、署名者が文字を書く際の筆圧の変化にもとづいて署名者の認証を行うこともできる。その際、液晶モニター８の表示部に筆圧センサーを重ねて配置すれば、署名者は小切手などの画像の署名欄にモニター上で署名すれば認証が行われることになり、認証方法が署名者にとって分かり易いものとなる。図３は、このような構成の電子署名装置３０の一例を示す外観図である。液晶モニター８の表示部３２に、透明なパネル状の筆圧センサー３４が重ねて配置されており、署名者はこの上でサインを行えばよい。

【００２１】そして、キーボードなどのパスワード入力手段を設け、入力されたパスワードと、あらかじめ登録されているパスワードとを、照合手段としてのたとえばＣＰＵ１４により比較して認証を行う構成とすることも可能である。また、単一の認証手段にかぎらず、複数の認証手段を組み合わせて用いることも有効である。

【００２２】本実施の形態例では、情報出力手段として液晶モニター８を用いたが、文書の内容を読み上げて署名者に通知する構成としてもよい。図４はこのような構成の他の実施の形態例を示す外観図でる。図４に示した電子署名装置３６では、液晶モニター８に代えてスピーカー３８が配置されており、スピーカー３８を通じて署名すべき文書の内容が音声情報として出力される。署名者はこの音声を聴取して文書の内容を確認し、署名を行うことができる。なお、スピーカー３８の代わりにイアホーンをも用いることも無論可能である。

【００２３】さらに、情報出力手段として、署名すべき文書データーを映像信号として出力する出力端子や、文書データーを音声信号として出力する出力端子を設け、実際に画像を表示したり、音声を発する機器は外部に接続するようにすることも可能である。また、電子署名装置２ではパソコンなどの外部機器との接続をＵＳＢ方式により行うとしたが、ＲＳ２３２Ｃ規格にもとづくインターフェースを用いることも無論可能である。

【００２４】

【発明の効果】以上説明したように本発明の電子署名装置では、情報出力手段が、電子署名を行うべきデーターを表す情報を出力するので、署名者はこの出力結果にもとづいて電子署名を行うべきデーターの内容を確認する

7

ことができる。そして、ハッシュ値生成手段は上記電子署名を行うべきデーターにもとづいてハッシュ値を生成する。その後、ハッシュ値暗号化手段は、暗号鍵生成手段が生成した秘密鍵を用いてハッシュ値生成手段が生成したハッシュ値を暗号化し、ハッシュ値出力手段は、署名者が特定の人物であると認証手段が判定した場合に、ハッシュ値暗号化手段が暗号化したハッシュ値を出力する。このように本発明では、情報出力手段が内容確認のために情報を出力するデーターと、ハッシュ値生成手段がハッシュ値の生成に用いるデーターとは常に同一であり、したがって、かならず署名者が確認したデーターに対してのみ電子署名が行われる。

【図面の簡単な説明】

【図１】本発明による電子署名装置の一例を示すブロック図である。

【図２】（Ａ）は実施の形態例の電子署名装置を示す外観図、（Ｂ）は液晶モニターに表示された小切手を示す平面図である。

【図３】筆圧センサーを用いた実施の形態例を示す外観図である。

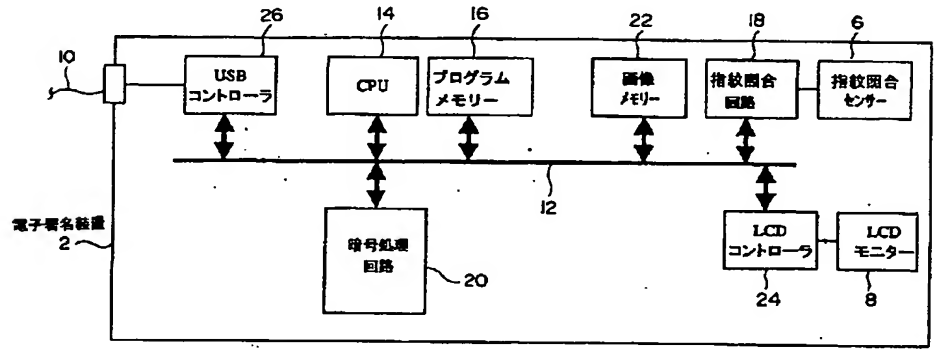
【図４】スピーカーを用いた実施の形態例を示す外観図である。

【図５】従来の電子署名装置の一例を示す構成図である。

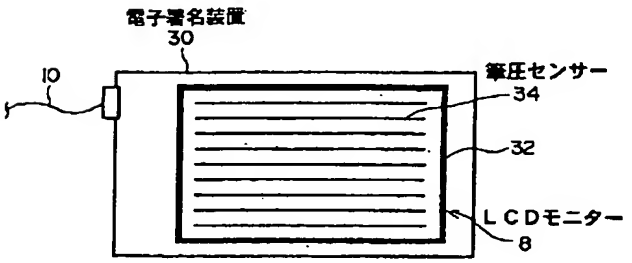
【符号の説明】

２……電子署名装置、４……装置収容体、６……指紋照合センサー、８……液晶モニター、１０……ＵＳＢケーブル、１２……バスライン、１４……ＣＰＵ、１６……プログラムメモリー、１８……指紋照合回路、２０……暗号処理回路、２２……画像メモリー、２４……液晶コントローラー、２６……ＵＳＢコントローラー、２８……指、３０……電子署名装置、３２……表示部、３４……筆圧センサー、３６……電子署名装置、３８……スピーカー、１０２……電子署名装置、１０４……指紋照合器、１０６……パーソナルコンピュータ（パソコン）、１０８……小切手、１１０……指紋照合センサー、１１２……ケーブル。

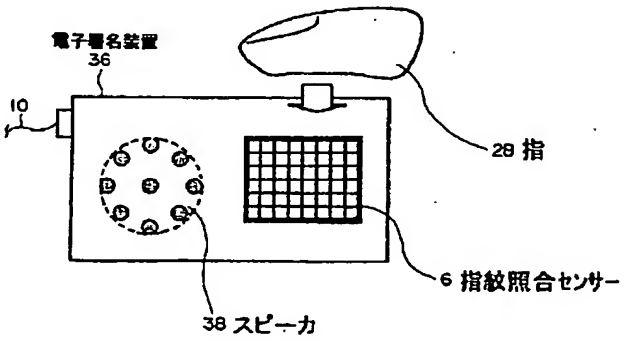
【図１】



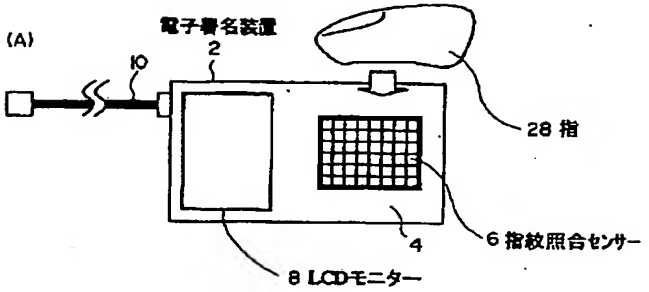
【図３】



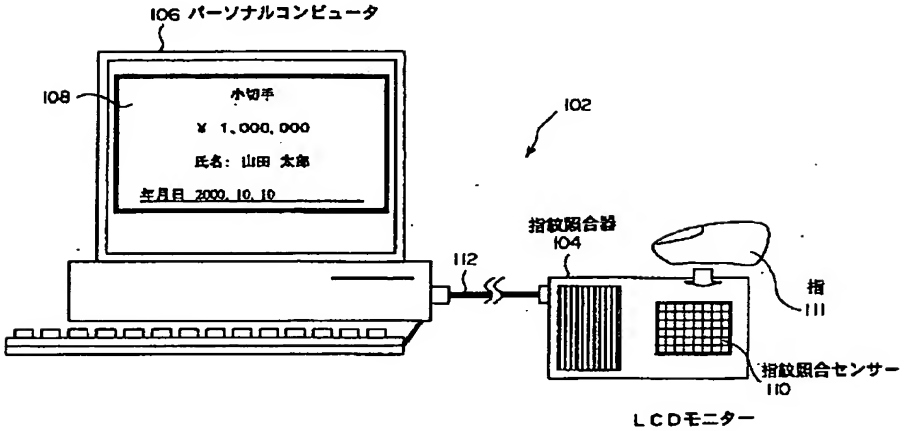
【図４】



【図２】


(A)
電子署名装置
2
10
28 指
6 指紋照合センサー
4
8 LCDモニター
(B)
8
小切手
¥ 1、000、000
氏名：山田 太郎
年月日 2000、10、10

【図５】


106 パーソナルコンピュータ
108
小切手
¥ 1、000、000
氏名：山田 太郎
年月日 2000、10、10
102
指紋照合器
104
112
指
111
指紋照合センサー
110
LCDモニター

(Translation) Mailed: June 14, 2005

NOTIFICATION OF REASON FOR REJECTION

Patent Application No.: 2005-045651

Examiner's Notice Date: June 8, 2005

Examiner: N. Ishida

This application is rejected on the grounds stated below. Any opinion about the rejection must be filed within THREE MONTHS of the mailing date hereof.

REASON

The invention(s) recited in the following claim(s) is unpatentable under Section 29 (2) of the Patent Law, as being such that the invention could easily have been made by a person with ordinary skill in the art to which the invention pertains, on the basis of the invention described in the following publication(s) distributed in Japan or a foreign country prior to this application.

REMARKS

References Cited:
1. Jpn. Pat. Appln. KOKAI Publication No. 2002-258745
2. PCT International Publication No. 03/102788
3. PCT International Publication No. 02/46904

Reference 1 is applicable to claims 1, 6, 11, 12, 16, 18, 19, 25 and 26.

Reference 1 describes a portable data storage device ("electronic signature device") comprising a non-volatile memory ("program memory") for storing user data ("document data"), an interface section ("USB controller") for receiving data from and transmitting data to a host ("personal computer"), a master control unit ("CPU") for transferring data to and from the non-volatile memory, and integrated circuit means ("code processing circuit") for generating at least one key ("private key" or "public key"), the device being arranged, upon receiving a command from a host requesting data, to transmit the requested data stored in its memory to the host using the interface section, and to transmit a key generated by the integrated circuit means to the host using the interface section (refer to paragraphs [0009]-[0017] and FIG. 1).

In general, a digital signature is transmitted together with data to which the signature is affixed and a key for verifying the signature. Therefore, a person with ordinary skill in the art could have easily come up with the inventions of claims 1, 6, 11, 12, 16 and 18, by transmitting "document data" and "public key" to a personal computer, together with a "digital signature".

Reference 1 is applicable to claims 2-5, 17 and 20-24.

In general, selecting whether to produce a digital signature at a device or at a host is a matter of design choice. A person with ordinary skill in the art can easily select whether to produce a digital signature at a device or at a host, according to the calculation performance of the device and the host. A private key used for producing a digital signal should be safely distributed from where the key has been generated, in accordance with the selection result. Accordingly, there is no particular difficulty in achieving the inventions of claims 2-5 by safely distributing the "private key", described in Reference 1, from an "electronic signature device" to a "personal computer", and verifying the produced digital signature using the "electronic signature device" comprising a "public key".

Reference 1 is applicable to claims 7, 9, 27 and 29.

Reference 1 describes certifying the signer using a finger print recognition sensor and a finger print recognition circuit (refer to paragraph [0015]).

Reference 1 is applicable to claims 8 and 28.

The technique of encrypting confidential data for transmission and reception, is well-known. Therefore, there is not particular difficulty in achieving the inventions of claims 8 and 28 by transmitting and receiving the "document data", described in Reference 1, after encoding the data.

References 1 and 2 are applicable to claims 10 and 30.

Reference 2 describes a portable memory device having a data compression/decompression engine for compressing/decompressing write/read data (refer to page 2, line 15 to page 3, line 16 and FIG. 1). Thus, there is no particular difficulty in providing the data compression/decompression engine to the electronic signature device, described in Reference 1, to achieve the structures of the inventions of claims 10 and 30.

Reference 1 is applicable to claim 13.

In general, selecting what type of interface to provide between a host and a device is a matter of design choice to a person with ordinary skill in the art. Further, it is well-known to use wireless communication as the interface between a host and a device. Therefore, there is no particular difficulty in achieving the invention of claim 13 by using wireless communication as the interface between the personal computer and the electronic signature device, described in Reference 1.

References 1 and 3 are applicable to claim 14.

Reference 3 describes a mouse with a USB storage device mounted within a housing of a USB mouse (refer to page 4. lines 9-14 and FIG. 1). There is no particular difficulty in achieving the invention of claim 14 by applying this technique to the electronic signature device, described in Reference 1, so as to provide an integral structure of the electronic signature device and a mouse as a one-piece structure.

Reference 1 is applicable to claim 15.

Selecting what type of data is to store in the program memory of Reference 1 is

a matter of design choice to a person with ordinary skill in the art.